JAY CLAYTON
United States Attorney for the
Southern District of New York
By: Tara La Morte
Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007
(212) 637-1041

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, -v.- 286,383.398942 USDC CURRENTLY HELD WITHIN THE FOLLOWING VIRTUAL CURRENCY ADDRESS ON THE ETHEREUM BLOCKCHAIN: 0xfae5a6D3bD9BD24a3ED2f2A8A6031C83976c19a2 Defendant-*in-rem*.	VERIFIED CIVIL COMPLAINT FOR FORFEITURE 25 Civ. 4107

Plaintiff United States of America, by its attorney, Jay Clayton, United States Attorney for the Southern District of New York, for its verified civil complaint, alleges, upon information and belief, as follows:

I. JURISDICTION AND VENUE

1. This action is brought pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 984(a)(1)(A) by the United States of America seeking the forfeiture of the following:

a. 286,383.398942 USDC currently held within the following virtual currency address on the Ethereum Blockchain: 0xfae5a6D3bD9BD24a3ED2f2A8A6031C83976c19a2

(collectively, the "Defendant-*in-rem*").

2. This Court has original jurisdiction over this forfeiture action pursuant to Title 28, United States Code, Sections 1345 and 1355.

3. Venue is proper pursuant to Title 28, United States Code, Section 1355(b)(1)(A) because the acts and omissions giving rise to the forfeiture took place in the Southern District of New York.

4. As set forth below, there is probable cause to believe that the Defendant-*in-rem* is subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) as proceeds traceable to the commission of violations of Title 18, United States Code, Section 1343 (wire fraud), and Section 981(a)(1)(A) as involved in violations of Title 18, United States Code, Section 1956 (money laundering).

II. PROBABLE CAUSE FOR FORFEITURE

5. This action arises out of an investigation conducted by law enforcement authorities (the "Investigation") into victims of a scheme in which the scheme's perpetrators deceived victims into sending cryptocurrency to the perpetrators by inducing the victims to enter their cryptocurrency wallet credentials on "spoofed" domains, and then using those

credentials to access and launder the contents of the victims' wallets (the "Scheme"). The Investigation has discovered that one such Ethereum address used to effect the Scheme is the virtual currency address on the Ethereum Blockchain: 0xfae5a6D3bD9BD24a3ED2f2A8A6031C83976c19a2 (the "Target Address"). The Investigation has revealed that the 286,383.398942 USDC that is currently held within the Target Address represents proceeds of the Scheme and is thus subject to forfeiture.

CRYPTOCURRENCY BACKGROUND

6. A cryptocurrency is a decentralized virtual currency, exchangeable against fiat currency via online platforms that serve as exchangers. Many cryptocurrency transactions are peer-to-peer. Cryptocurrencies are maintained in virtual "wallets" containing "addresses," which are represented by a unique series of alpha-numeric characters. All cryptocurrency transactions, both incoming and outgoing, are recorded in a publicly-available ledger called a "blockchain," which records every address that has ever transferred or received a unit of a given cryptocurrency. Ethereum is one example of a blockchain. An "Ethereum address" can hold multiple cryptocurrencies that are compatible with the Ethereum blockchain, including but not limited to USDC.

7. Blockchains, like the Ethereum blockchain, serve as vast open ledgers for any individual to examine. Thus, all transactions are completely transparent in that any transfer can be verified or monitored on the publicly-available blockchain. However, in most blockchains, the senders and receivers are largely anonymous. The sender and receiver in a given transaction are each represented by their cryptocurrency address, an alpha-numeric string analogous to a traditional bank account number.

8. Cryptocurrencies can be stored both online and offline. They can be stored in accounts operated by a host of various providers and accessed via devices capable of connecting to the internet. However, this access to the internet also means that such online accounts are more vulnerable to thefts. Thus, cryptocurrency can also be stored in "cold storage," which refers to the offline holding of the funds. Cold storage methods include, for example, a USB drive, a specialized hardware wallet, which typically resemble a handheld USB drive, or even on a piece of paper.

9. Stablecoins are a type of virtual currency. They may be pegged to a currency, such as the United States dollar, or to a commodity's price, such as gold. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

10. The USDC stablecoin was created by Centre, an organization founded by the companies Coinbase and Circle. Circle is currently the sole entity involved in the management of USDC tokens and serves as its treasury. As relayed by Circle, USDC is backed by highly liquid cash and cash-equivalent assets and is redeemable 1:1 for United States dollars. Customers can redeem USDC for its United States dollar equivalent by depositing its USDC with Circle. When USDC is redeemed, it is taken out of circulation, a process known as "burning".

THE DEFENDANT-*IN-REM*

11. As a result of the Investigation, the Investigation learned the following:

a. The Victim is the owner of the following Ethereum address: 0xaab96f14cf3c051759ce95a9b44acb93cccaecd1 (the "Victim Address"), which is

contained in a cryptocurrency wallet controlled by the Victim. On or about November 15, 2021, the Victim's wallet contained several different cryptocurrencies, including Olympus, Wonderland, Klima DAO, Hector DAO, Dai, and Fantom. The total value of the cryptocurrencies contained in the Victim Address immediately prior to November 15, 2021, was equivalent to approximately $300,000.

b. On or about November 15, 2021, the Victim sought to access through his cellular phone the cryptocurrency exchange SpookySwap,[1] which the Victim had accessed and used previously from his desktop. The Victim used his cellular phone to access the Google search engine, performed a search, and clicked on the first result, which was a Google advertisement for SpookySwap. The Victim arrived at the website. At that time, the Victim's Metamask[2] wallet was not connected to the exchange, which the Victim believed was not unusual as it was the first time he was logging on to Spookyswap through his cellular phone.

c. Next, a square pop-up in the middle of the screen displayed, "Connect a Wallet" and the Victim clicked the link. An additional popup required entry of a "seed phrase"[3], which the Victim entered and then clicked "Proceed".

d. At this point nothing happened, despite the Victim refreshing

1 SpookySwap is an automated exchange for a variety of cryptocurrencies. It can be accessed using the following URL: spookyswap.finance.

2 Metamask is a free mobile and web crypto wallet that allows users to store, swap and interact with cryptocurrencies.

3 Typically, a "seed phrase" is comprised of a set of 12 to 24 seemingly random words that represent a human readable form of the master private key from which the public and private cryptographic key pairs for that wallet are generated.

the website several times. The Victim logged on to Spookyswap from his desktop to check if the exchange was operational. From his desktop, the Victim observed that his Metamask wallet was already connected.

e. The Victim then observed that quantities of several different cryptocurrencies were transferred out of his wallet.

f. As of November 15, 2021, the total value of the cryptocurrencies missing from Victim's wallet was approximately $300,000.

g. The Investigation learned that the URL the Victim had accessed via the Google search on his cellular phone, which he believed to be "spookyswap.finance", was in fact "spookysvwap.finance"[4], a "spoofed" domain meant to trick visitors by appearing nearly identical to the legitimate domain.

12. A review of the activity recorded on the Ethereum blockchain regarding the Victim Address revealed the following:

a. At approximately 5:45 a.m. UTC on November 15, 2021, numerous outbound transfers of the cryptocurrencies contained in the Victim Address were received by two other Ethereum addresses: Ox35663B9A8e4563EeFdf852018548b4947B20fCe6 ("Subject Address-1") and Oxf64e1c5b6e17031f5504481ac8145f4c3eab4917 ("Subject Address-2", and together the "Subject Addresses");

b. Over the course of the next several hours, the contents of Subject Addresses were ultimately converted from the cryptocurrencies that had been stored in the Victim Wallet to USDC;

4 As of December 21, 2021, spookysvwap.finance is not an active URL.

c. The contents of Subject Address-2 were ultimately transferred into Subject Address-1; and

d. After this transfer, the entire sum of cryptocurrency stolen from the Victim Address was contained in Subject Address-1 as USDC.

13. A review of the activity recorded on the blockchain regarding Subject Address-1 revealed the following:

a. Beginning at approximately 2:30 AM on November 16, 2021, 286,383.398942 USDC was transferred out of Subject Address-1 and ultimately received by the Target Address.

14. A detailed explanation of the tracing of the funds stolen from the Victim to The Target Address is set forth in Appendix A, which is incorporated by reference herein. As set forth in Appendix A, based on the timing of the transfers and the amounts in the wallets prior to the transfers being made, 286,383.398942 USDC in the Target Address is directly traceable to the cryptocurrency stolen from the Victim.

15. The Defendant-in-rem is currently frozen and held in the Target Address.

III. CLAIMS FOR FORFEITURE

Count One

Forfeiture Under 18 U.S.C. § 981(a)(1)(C)
(Property Constituting or Derived from Proceeds Traceable to a Violation of 18 U.S.C. § 1343 or Property Traceable to Such Property)

16. Paragraphs 1 through 15 of this Complaint are repeated and re-alleged as if fully set forth herein.

17. Pursuant to Title 18, United States Code Section 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of any offense constituting "specified unlawful activity" as defined in section 1956(c)(7) of this title, or a conspiracy to commit such offense, is subject to forfeiture.

18. As set forth above, for purposes of Section 1956, "specified unlawful activity" includes wire fraud, in violation of 18 U.S.C. § 1343.

19. By reason of the foregoing the Defendant-*in-rem* is subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) as property constituting or derived from proceeds traceable to a violation of Title 18, United States Code, Section 1343.

Count Two

Forfeiture Under 18 U.S.C. § 981(a)(1)(A)
(Property Involved in a Transaction In Violation of 18 U.S.C. § 1956 or Property Traceable to Such Property)

20. Paragraphs 1 through 15 of this Complaint are repeated and re-alleged as if fully set forth herein.

21. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property, is subject to forfeiture.

22. For purposes of Section 1956, "specified unlawful activity" includes wire fraud, in violation of 18 U.S.C. § 1343.

23. As set forth above, the Defendant-*in-rem* was involved in or was traceable to property involved in transactions or attempted transactions in violation of 18 U.S.C. §1956(a)(1)(B)(i), to wit, perpetrators of the Scheme, knowing that the Defendant-*in-rem* represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct financial transactions, which transactions affected interstate and foreign commerce, and which in fact involved the proceeds of specified unlawful activity, to wit, the wire fraud Scheme described above, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of the Scheme, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

24. By reason of the foregoing the Defendant-*in-rem* is subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(A) as property involved in violations of Title 18, United States Code, Section 1956, or property traceable to such property.

WHEREFORE, plaintiff United States of America prays that process issue to enforce the forfeiture of the Defendant-*in-rem* and that all persons having an interest in the Defendant-*in-rem* be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendant-*in-rem* to the United States of America for disposition according to law, and that this Court grant plaintiff such further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: New York, New York
May 15, 2025

JAY CLAYTON
United States Attorney for the
Southern District of New York
Attorney for the Plaintiff
United States of America

By: _____

Tara La Morte
Assistant United States Attorney
One St. Andrew's Plaza
New York, New York 10007
Telephone: (212) 637-1041

Appendix A

Time is in UTC

On November 15, 2021:

i. At approximately 5:43 AM, 26,485.470867 DAI and 10,200 FTM were transferred from the Victim Address to 0x35663b9a8e4563eefdf852018548b4947b20fce6 ("0x3566" referenced above as Subject Address-1) on the Fantom blockchain.
ii. At approximately 5:44 AM, 612.404113 HEC was transferred from the Victim Address to 0x3566 on the Fantom blockchain.
iii. At approximately 5:47 AM, 0x3566 swapped 612.404113 HEC for 130,001.0644698 DAI.
iv. At approximately 5:48 AM, 0x3566 swapped 10,200 FTM for 26,182.57113709 DAI.
v. At approximately 5:48 AM, the Victim Address sent 6.062080564 TIME to 0xf64e1c5b6e17031f5504481ac8145f4c3eab4917 (referenced above as Subject Address-2). The TIME was swapped for 517.750756 AVAX and returned to the Victim Address on the Avalanche blockchain.
vi. At approximately 5:48 AM, 518 AVAX was sent from the Victim Address to 0x3566 on the Avalanche blockchain.
vii. At approximately 5:49 AM, 53.831005 HEC was transferred from the Victim Address to 0x3566 on the Fantom blockchain.
viii. At approximately 5:50 AM, 0x3566 swapped 53.831005 HEC for 11,498.929671 DAI.
ix. At approximately 5:51 AM, 21.09532188 Olympus was sent from the Victim Address to 0x3566 on the Ethereum blockchain.
x. At approximately 5:52 AM, 14.49676657 Klima was sent from the Victim Address to 0x3566 on the Polygon blockchain.
xi. At approximately 5:53 AM, 0x3566 sent 194,168.036145 DAI to the Multichain bridge.
xii. At approximately 5:53 AM, 193,973.86810926 DAI exits the Multichain bridge and is sent to 0x3566 on the Ethereum blockchain.
xiii. At approximately 5:54 AM, 0x3566 swapped 518.666874 AVAX for 51,111.317443 USDC.e and sent across the Avalanche bridge.[1]
xiv. At approximately 5:54 AM, 51,057.581972 USDC exited the Avalanche bridge and was sent to 0x3566 on the Ethereum blockchain.
xv. At approximately 5:56 AM, 0x3566 swapped 22.32840895 Klima for 36,003.105021 USD Coin (PoS)
xvi. At approximately 5:57 AM, 0x3566 sent 36,003.105021 USD Coin (PoS) across the Polygon Bridge.
xvii. At approximately 5:59 AM, 0x3566 swapped 21.09532188 Olympus for 18,063.414306 USDC.
xviii. At approximately 7:22 AM, 0x3566 swapped 193,973.868109 DAI for 193,887.310853 USDC.

xix. At approximately 10:28 AM, 36,003.105021 USDC exited the Polygon Bridge and was sent to 0x3566 on the Ethereum blockchain.

On November 16, 2021:

i. At approximately 2:44 AM, 0x3566 sent 21,000 USDC to the Target Address. Prior that transfer, the balance of USDC in 0x3566 was 621,953.254772.5
ii. At approximately 10:12 AM, 0x3566 sent 15,000 USDC to 0x5fb1ff8c5c515b10f6171c4cb2736f65688c0027 ("0x5fb1"). At approximately 10:22 AM, 0x5fb1 sent 15,000 USDC to the Target Address.
iii. At approximately 1:40 PM, 0x3566 sent 613,076.001375 USDC to 0x029c2c986222dca39843bf420a28646c25d55b6d ("0x029c"). Prior that transfer there was no USDC in 0x029c. The next transaction from 0x029c was at approximately 4:26 PM, when 0x029c sent 600,000 USDC to the Target Address.

In Summary:

i. The HEC, DAI, and FTM tokens from the Victim Address were converted to 193,887.310853 USDC.
ii. The Klima tokens from the Victim Address were converted to 23,375.0918106 USDC.
iii. The AVAX tokens from the Victim Address were converted to 51,057.581972 USDC.
iv. The Olympus tokens from the Victim Address were converted to 18,063.414306 USDC.
v. Therefore, the total amount of USDC sent to 0x3566 (i.e. Subject Address-1) on the Ethereum blockchain attributable to the Victim is 286,383.398942. Prior to the first deposit of USDC into 0x3566 referenced above (November 15, 2021, at 5:54 AM), the balance in USDC in 0x3566 was 177,701.328635. During the timeframe between that first deposit into 0x3566 (November 15, 2021, at 5:54 AM) and the last outgoing transfer of USDC from 0x3566 to 0x029c) described above (November 16, 2021, at 1:40 PM), there was an additional 179,363.260588 in USDC deposited into 0x3566 from other sources not attributable to the Victim.

VERIFICATION

STATE OF NEW YORK)
COUNTY OF NEW YORK :
SOUTHERN DISTRICT OF NEW YORK)

Gregory Dunlavey, being duly sworn, deposes and says that he is a Deputy Chief Investigator with the New York County District Attorney's Office, and as such has responsibility for the within action; that he has read the foregoing complaint and knows the contents thereof, and that the same is true to the best of his knowledge, information, and belief.

The sources of deponent's information and the ground of his belief are official records and files of the New York County District Attorney's Office and the United States Secret Service, and information obtained by the deponent and other law enforcement officials, during an investigation of alleged violations of Title 18 of the United States Code.

Gregory Dunlavey
Deputy Chief Investigator
New York County District Attorney's Office